Claims

What is claimed is:

1. A method for providing enhanced privacy in an RFID system comprising a plurality of RFID devices, each having an associated identifier, and at least one reader which communicates with one or more of the devices, the method comprising the steps of:

receiving in a blocker device a communication directed from the reader to one or more of the RFID devices; and

generating in the blocker device an output transmittable to the reader, the output simulating one or more responses from at least one of the RFID devices in a manner which prevents the reader from determining at least a portion of the identifier of at least one of the RFID devices.

2. The method of claim 1 wherein the blocker device comprises one of the RFID devices.

3. The method of claim 1 wherein the output transmittable to the reader is generated in the blocker device based at least in part on information in the received communication.

4. The method of claim 1 wherein the output simulates responses from multiple ones of the RFID devices.

5. The method of claim 1 wherein the blocker device generates the output in such a manner that the reader is prevented from determining identifiers for only those of the RFID devices having identifiers within a designated privacy zone.

6. The method of claim 5 wherein at least one of the RFID devices has an identifier which is modifiable such that the identifier is transferable from outside the privacy zone to within the privacy zone upon the occurrence of a specified event.

7. The method of claim 5 wherein at least one of the RFID devices has an identifier which is modifiable such that the identifier is transferable from within the privacy zone to outside the privacy zone upon the occurrence of a specified event.

8. The method of claim 1 wherein the reader utilizes a singulation algorithm to determine the identifiers of the RFID devices.

9. The method of claim 8 wherein the singulation algorithm comprises a tree-walking singulation algorithm.

10. The method of claim 9 wherein the communication from the reader comprises a query specifying at least a subset of the identifiers, and further wherein the blocker device first determines if any of the identifiers in the subset are within a designated privacy zone, and if so generates the output simulating one or more responses from at least one of the RFID devices.

11. The method of claim 9 wherein the output simulating one or more responses from at least one of the RFID devices comprises a broadcast of a signal representing the presence of RFID device identifiers at least one of which carries a '0' bit in a given position and at least one of which carries a '1' bit in the same position.

12. The method of claim 8 wherein the singulation algorithm comprises an ALOHA singulation algorithm.

13. The method of claim 12 wherein the communication from the reader comprises a query involving a selection set specification, and further wherein the blocker device first determines if an identifier in a designated privacy zone has at least a portion thereof corresponding to the selection set specification, and if so generates the output simulating one or more responses from at least one of the RFID devices.

14. The method of claim 12 wherein a privacy zone P is specified in terms of a set of arbitrary-length prefixes $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$, and wherein the blocker device generates the output only if a selection mask σ specified by the reader is such that σ_i is a prefix of σ or vice versa.

15. The method of claim 12 wherein the communication from the reader comprises a communication designating a particular time slot, and further wherein the blocker device first determines if there exists an identifier in a designated privacy zone such that a function of the identifier evaluates to the particular time slot, and if so generates the output simulating one or more responses from at least one of the RFID devices within the particular time slot.

16. The method of claim 15 wherein the generated output simulates collisions in every time slot s for which $s = f(R, T, S)$, where f is the function, R denotes a random or pseudorandom value, T denotes an identifier in a privacy zone P, and S denotes a slot allocation of the ALOHA singulation algorithm.

17. The method of claim 1 wherein the blocker device comprises a full blocker tag and the generated output simulates all possible identifiers for a given set of RFID devices.

18. The method of claim 1 wherein the blocker device comprises a selective blocker tag and the generated output simulates responses of only a subset of all possible identifiers for a given set of RFID devices.

19. The method of claim 1 wherein the blocker device communicates to the reader information specifying a particular subset of a given set of RFID devices for which the reader will be unable to singulate identifiers.

20. The method of claim 1 wherein the blocker device is configured to communicate to the reader information specifying a particular selective blocking policy being implemented by the blocker device.

21. The method of claim 20 wherein the system supports a number of virtual identifiers denoted $t, t + 1, \ldots, t + k$, each corresponding to one of a plurality of selective blocking policies $0, 1, \ldots, k$, and further wherein the blocker device communicates to the reader that it is implementing a particular selective blocking policy i by generating the output so as to simulate a response from an RFID device having identifier $t + i$.

22. The method of claim 20 wherein a designated prefix σ^* is utilized to identify any of the devices configured to implement a selective blocking policy, the reader determining any devices so configured by issuing a query having a selection mask corresponding to the designated prefix σ^*.

23. The method of claim 20 wherein the blocker device has an identifier of the form $T_i = \sigma^* \parallel \rho_i \parallel P_i$, where $\parallel$ denotes string concatenation, ρ_i denotes a random value specific to the blocker device, and P_i denotes the selective blocking policy implemented by the blocker device.

24. The method of claim 1 wherein the reader is operative to detect the presence of the blocker device, and to determine if the blocker device is operating as a selective blocker device or a full blocker device.

25. The method of claim 1 wherein the reader is operative to detect the presence of the blocker device by determining if a number of perceived RFID device identifiers exceeds a specified threshold.

26. The method of claim 1 wherein the reader is operative to detect the presence of the blocker device by accessing a database listing valid identifiers in a given range of RFID device

identifiers, and determining that the blocker device is present upon detection of an RFID device having an identifier not in the database of valid identifiers.

27. The method of claim 1 wherein the reader is operative to detect the presence of the blocker device by interacting with one or more other readers to determine information specifying the physical locations of at least a subset of the RFID devices, and processing the determined location information to ascertain if the blocker device is present.

28. The method of claim 1 wherein the blocker device is configurable such that a privacy policy implemented by the blocker device is selectable responsive to a command.

29. An apparatus for providing enhanced privacy in an RFID system, the system comprising a plurality of RFID devices, each having an associated identifier, and at least one reader which communicates with one or more of the devices, the apparatus comprising:

a blocker device operative to receive a communication directed from the reader to one or more of the RFID devices, and to generate an output transmittable to the reader, the output simulating one or more responses from at least one of the RFID devices in a manner which prevents the reader from determining at least a portion of the identifier of at least one of the RFID devices.

30. An RFID system comprising:

a plurality of RFID devices, each having an associated identifier; and

at least one reader which communicates with one or more of the devices;

wherein a blocker device is operative to receive a communication directed from the reader to one or more of the RFID devices, and to generate an output transmittable to the reader, the output simulating one or more responses from at least one of the RFID devices in a manner which prevents the reader from determining at least a portion of the identifier of at least one of the RFID devices.

31. An apparatus for providing enhanced privacy in an RFID system, the system comprising a plurality of RFID devices, each having an associated identifier, the apparatus comprising:

at least one reader which communicates with one or more of the devices;

wherein a blocker device of the system is operative to receive a communication directed from the reader to one or more of the RFID devices, and to generate an output transmittable to the reader;

wherein the reader is configured to receive from the blocker device information specifying a particular selective blocking policy being implemented by the blocker device.